NASA Procedural Requirements

NPR 1600.3
Effective Date: May 31, 2012
Expiration Date: May 31, 2017

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Personnel Security (Change 2, April 29, 2013)

Responsible Office: Office of Protective Services

Chapter 3. Personnel Security Investigations for National Security Positions

3.1 General

3.1.1 National security requires each agency to follow established procedures to identify national security positions. Positions identified by this process within NASA require regular use of or access to classified information, or to occupy a sensitive position. This chapter addresses the sensitivity designation program associated with national security, the criteria for determining national security sensitivity levels, and investigation type screenings.

3.1.2 Position sensitivity designation is based on an assessment of the degree of damage that an individual, by virtue of the occupancy of a national security position, could cause to national security.

3.1.3 Investigations are conducted to provide a basis for ensuring that the granting of a security clearance to an individual is clearly consistent with the interests of national security.

3.1.4 Personnel security reports and records shall be handled in accordance with the Privacy Act of 1974.

3.1.5 OPM conducts a range of investigations that satisfy the various requirements for the three position-sensitivity levels described in this chapter, as they relate to accessing CNSI.

3.1.6 NASA contracts requiring the generation of and/or access to CNSI shall be processed in accordance with the requirements of EO 12829, the National Industrial Security Program Operating Manual (NISPOM) and NISPOM Supplement.

3.2 Scope

3.2.1 This chapter prescribes the procedures whereby NASA Federal employees are selected, processed, investigated, and adjudicated for national security positions, consistent with adjudicative guidelines contained in White House Memorandum, Adjudicative Guidelines, dated, December 29, 2005, and the OPM's Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide.

3.2.2 This chapter applies to contractor employees providing services under a NASA classified contract that requires access to Sensitive Compartmented Information (SCI).

3.3 Program Oversight

As part of its responsibility for the functional management and oversight of the NASA Personnel Security Program, OPS shall verify compliance with personnel security clearance requirements when conducting functional reviews or periodic audits of Center security programs.

3.4 Principles of Personnel Security Clearance Management

3.4.1 The purpose of the personnel security clearance program is to ensure that only loyal, trustworthy, and reliable people are granted access to classified information or assigned to sensitive duties.

3.4.2 Due to the cost and time invested in conducting the appropriate investigation, managers and supervisors should be judicious and accurate in determining an employee's position sensitivity and need for access to CNSI. Managers and supervisors should establish the access requirement during the development of the individual position description and assign the appropriate designation of position risk and sensitivity level for each NASA position description. Failure to properly identify upfront the need for access to CNSI causes added expense that will be borne by the program and results in unnecessary delays.

a. Managers and supervisors should discuss with the employee their responsibilities and obligations in handling CNSI prior to initiating a new PSI for access to CNSI.

3.4.3 The requirement for access to CNSI shall be clearly established during submission of the NF 1630, Request for Access to CNSI and the position description development phase. Once the position has been determined to require access to CNSI and position sensitivity has been assigned, the new appointee must complete the SF 86 in e-QIP.

3.4.4 Access to CNSI shall not be requested or granted solely to permit entry to, or ease of movement within NASA controlled areas, other Government agency facilities, or contractor facilities when the individual involved has no need for access to classified information.

3.4.5 Requests for security clearances shall not be processed or granted based merely on a speculative need for access or as a result of any particular grade, position, or affiliation. Requesting security clearances for contingency purposes in excess of actual official requirements is prohibited.

3.4.6 The level at which access to CNSI is requested and granted shall be clearly documented on the NF 1630, Request for Access to Classified National Security. Access to CNSI must be limited and should relate directly to the level of classified information for which access is clearly justified in the performance of official duties and for which the individual has a demonstrated "need to know."

3.4.7 PSI and eligibility determination shall be mutually and reciprocally accepted by all agencies unless an agency has substantial information indicating an employee may not satisfy the access eligibility standards.

a. Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations. They may also be reinvestigated at any time, if there is reason to believe that they may no longer meet the standards for access.

3.4.8 A person may have access to classified information provided that:

a. A favorable determination of eligibility for access has been made by an agency head or the agency head's designee; and

b. The person has executed an SF 312; and

c. The person has a need-to-know the information.

3.4.9 The Center security office will notify the employee in writing when an interim or final clearance eligibility decision has been made, or a reciprocal clearance has been accepted. The Center security office shall conduct all required orientation training as well as ensure the execution, witness, acceptance, and storage of the SF 312 consistent with 32 C.F.R. pt. 2003.20, Classified Information Nondisclosure Agreement: SF 312.

3.4.10 Every person who has met the standards for access to classified information will receive training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

3.4.11 An annual review of clearance and access requirements is necessary to ensure Center personnel security clearance needs are properly managed. The CCS/CCPS will develop and implement the appropriate local procedures necessary to ensure a viable review is conducted.

3.4.12 Personnel with clearances who have not had the need to access CNSI during the previous year will be given serious consideration for administrative withdrawal of their clearance as determined by supervisors during the revalidation process.

3.4.13 Clearances will not be retained merely as a stop-gap measure in the event the holder may need access to CNSI. A clear demonstrable operational requirement is necessary to possess the clearance as annotated in the position description.

3.4.14 Results of the favorable adjudication determination will be posted and made available to Center security personnel via the NASA Clearance Tracking System (NCTS).

3.5 Sensitive Compartmented Information (SCI)

3.5.1 Candidates for SCI access shall have a favorably adjudicated Top Secret (TS) investigation.

3.5.2 Requests for access to SCI require the submittal of Form 2018A, Special Access Request Form.

3.5.3 The Form 2018A shall be prepared and justified by the employee's immediate supervisor. The line supervisor will submit it through the division director, or higher, depending on the applicant's organizational position, for review and approval. The request is then forwarded along with a copy of the employee's updated SF 86 to the HQ Special Security Office (SSO) for appropriate action.

3.5.4 A copy of the Form 2018A and the original signed SCI Non-Disclosure Form shall be retained by the SSO representative at the Center.

3.5.5 PSIs for access to classified information for individuals requiring TS, SCI, or Q (Department of Energy Restricted Data) clearance access are subject to periodic reinvestigations at any time following the completion of, but no later than five years from the date of, the previous investigation.

3.6 One-Time Access Determinations

3.6.1 Urgent operational requirements may occur where a NASA Federal employee in a non-sensitive position has a one-time or short duration requirement for access to CNSI at the Confidential or Secret level. Usually, the limited duration or nature of this access requirement does not warrant processing the individual for a personnel security investigation and final security clearance eligibility determination. One-time access determinations will not be granted for the TS level. One-time access determinations will be used sparingly and only under conditions of compelling Government need. CCS/CCPS or an official designated by the CCS/CCPS has the authority to grant one-time access determinations subject to the following terms and conditions.

3.6.2 One-time access determinations should not be issued more than three times to any person within a one calendar year time frame. The aggregate access will not exceed a total of 60 days accumulated during a single calendar year.

3.6.3 One-time access determinations shall only be granted to U.S. citizens that have been continuously employed by the Federal Government for the preceding 24 months.

3.6.4 If the need for access is expected to exceed 60 days, the individual will be processed for a final security clearance determination.

3.6.5 An individual requiring one-time access will complete a NASA Form 1630, Request for Access to CNSI, and have at least a favorable National Agency Check and Inquiries, or a criminal history and credit check with a favorable suitability determination and local records check. Such individuals will complete an SF 86 for review by a trained adjudicator.

3.6.6 An individual requiring one-time access to CNSI will execute an SF 312. The SF 312 shall be witnessed, accepted, and stored as required in Section 3.4.9 of this NPR.

3.6.7 One-time access determinations, subsequent debriefs, and any security clearance certification (i.e., one-time clearance granted from date-to-date) shall be properly documented in local Center security office files. NCTS shall not be used to document one-time access determinations.

3.7 Coding of Position Sensitivity Level Designation for National Security Positions

3.7.1 National security positions are designated as non-critical sensitive, critical sensitive, or special sensitive.

3.7.2 The proper coding of position sensitivity for national security positions is required on Position Description OF 8 and optional on the Notification of Personnel Action SF 50.

3.7.3 Center OHCM personnel are responsible for managing the Electronic Position Description System (e-PDS). They will coordinate in a timely manner with managers, supervisors, and the CCS/CCPS to accomplish sensitivity designation of positions for individuals requiring access to CNSI. After the appropriate position sensitivity determination has been assigned, the Center OHCM or OPS personnel will initiate the appropriate investigation in e-QIP.

3.7.3.1 Individuals in positions designated low risk that may have access to classified information will be vetted at the level commensurate with the clearance requirements. For example, a custodian serving in a position designated as low risk who works in an area with classified information would be processed on a SF 86 for an Access National Agency Check and Inquiries (ANACI) rather than a SF 85 or SF 85P to meet the appropriate scope of the investigation in support the clearance required. Guidance for designating position sensitivity levels is contained in Chapter 2.9 of this NPR.

3.7.4 SPECIAL-SENSITIVE (SS): Positions requiring access to Top Secret Sensitive Compartmented Information (TS/SCI) shall be designated Special-Sensitive and the individual will undergo a SSBI using Standard Form 86 (SF-86), and be favorably adjudicated prior to being granted access to TS/SCI.

3.7.4.1 Pre-appointment investigation requirements shall not be waived for positions designated SS.

3.7.5 SPECIAL ACCESS PROGRAM (SAP): Access to SAP information requires a current favorably adjudicated PSI for the appropriate classified level prior to being granted access to the information. National SAP requirements dictate that periodic reinvestigation shall be conducted every five years for all SAP personnel.

3.7.6 CRITICAL-SENSITIVE (CS): Positions requiring access to Top Secret (TS) or North Atlantic Treaty Organization (NATO) information will be designated critical-sensitive. Individuals in or selected for these positions shall undergo a SSBI, using SF-86, and be favorably adjudicated prior to being granted access to information.

3.7.7 NONCRITICAL-SENSITIVE (NCS): Positions requiring access to Secret, Confidential, or NATO Secret/Confidential information shall be designated noncritical-sensitive. New hires selected for these positions will undergo, at a minimum, an ANACI, using SF-86 in e-QIP, and be favorably adjudicated prior to being granted access to information.

3.7.8 Pre-appointment waivers from Center Human Resources Directors may be authorized by the AA, OPS to approve an emergency appointment or reassignment to a CS or NCS position prior to completion of the required pre-appointment investigation only when clear justification exists to warrant the waiver.

3.7.9 NON-SENSITIVE: Non-sensitive positions relate to any position that is not a national security position.

3.7.10 All NASA positions designated as testing designated positions (TDP) will be in accordance with EO 12564. Personnel holding active security clearances shall be entered into the Drug Testing Program for random testing.

3.8 Temporary/Interim Access to Classified National Security Information (CNSI)

3.8.1 Management officials are required to request temporary access eligibility for U.S. citizen employees, civil service employees, and/or consultants filling CS and NCS positions when essential and immediate operational requirements do not allow for waiting for a pending personnel security investigation to be completed and adjudicated.

3.8.2 Center security offices shall document requests and approvals for temporary access eligibility and will provide compelling justification to warrant access to CNSI in advance of formal investigation and adjudication. In all cases, the required personnel security investigation will be initiated, entered into NCTS, transmitted to OPM, and have a favorable NAC results prior to issuance of the interim Secret and Confidential clearance. All interim TS clearance requests shall be submitted to the AA, OPS, for approval.

3.9 Access to CNSI by Non-U.S. Citizens

3.9.1 Non-U.S. citizens (including lawful permanent residents (LPR)) are not eligible for a security clearance. However, under specific situations the AA, OPS, may authorize the granting of a Limited Access Authorization (LAA) to a non-U.S. citizen for specific information up to the Secret level when it has been determined that no U.S. citizen has the skills necessary to perform the work. The requesting organization shall submit a written request to the AA, OPS, via the CCS/CCPS. The request should:

a. Specify why it is impractical or unreasonable to use U.S. citizens to perform the required work or function.

b. Define the individual's special expertise.

c. Define the compelling reasons for the request.

d. Explain how access will be limited and physical custody of CNSI precluded.

e. Request concurrence or non-concurrence and forward it to the AA, OPS.

3.9.2. The AA, OPS, will coordinate with the Office of International and Intergovernmental Relations (OIIR) for concurrence and if approved, return it to the requestor. A copy shall be retained in the OPS CAF and CCS/CCPS files. The CCS/CCPS shall ensure:

a. A completed investigation and favorable adjudication is obtained before access is granted. The granting of interim or temporary access pending the completion of an investigation is prohibited.

b. Denied requests shall be returned to the requestor with an explanation of the denial.

c. Individuals with LAAs will be placed under closely controlled supervision of appropriately cleared persons (U.S. citizens). Managers will be made aware of access limits imposed on these individuals and shall ensure compliance with any restrictions imposed.

d. Individuals who have been granted an LAA shall not be allowed access to any classified information other than that specifically authorized under national disclosure policy. Additionally, physical custody of classified information by these individuals is not authorized.

e. Non-U.S. citizens are ineligible for access to intelligence information, communications security keying materials, TS information, Restricted or Formerly Restricted Data, Critical Nuclear Weapons Design Information (CNWDI), TEMPEST information, classified cryptographic information, or NATO classified information.

f. Requests for access to CNSI owned by another agency must be coordinated with and approved by that agency.

3.9.3 Access to classified information will be limited to that necessary to complete the task, and access shall be terminated upon completion of the task.

3.9.4 If the access request is initiated by a NASA-cleared contractor performing on a NASA classified contract, only the Defense Industrial Security Clearance Office (DISCO) or successor organization has the authority to grant access to a LAA to non-U.S. citizens. Procedures for coordination of the request are as follows:

a. A cleared contractor's Facility Security Officer will receive the endorsement of the CCS/CCPS, Center International Visitor Coordinator (IVC), Center Export Administrator (CEA), OIIR, and AA, OPS.

b. The CCS/CCPS will ensure the contract is current and evaluate the justification for the request. The non-U.S. citizen nominated for the LAA will sign a nondisclosure statement executed by the CCS/CCPS. The CCS/CCPS shall forward the completed package to the AA, OPS, for review, coordination, and endorsement.

c. If acceptable, the AA, OPS, shall endorse and return it to the contractor for forwarding to the DISCO. A completed SSBI and favorable adjudication is required before access is granted.

d. Denied requests shall be returned to the contractor with an explanation of the denial.

3.10 Reciprocal Recognition of Security Clearance Determinations

3.10.1 Acceptance of access eligibility determinations will be implemented in the following manner:

a. An employee with an existing security clearance (not including an interim clearance) who transfers or changes employment status is eligible for a security clearance at the same or lower level without additional or duplicative adjudication, investigation, or reinvestigation and without any requirement to complete or update a security questionnaire unless substantial information exists indicates that the standards may not be satisfied.

3.10.2 The "substantial information" exception to reciprocity recognition of security clearances does not authorize NASA personnel to request a new security questionnaire, review existing PSI questionnaires, or initiate new investigative checks (such as a credit check) to determine whether such substantial information exists.

3.10.3 Prior investigations shall be accepted reciprocally, provided the following conditions are met:

a. There has been no break in service in excess of 24 months; and

b. The prior investigation meets the required scope and coverage standards and is compatible with the sensitivity of the position; and

c. There has been no subsequent development of potentially disqualifying derogatory information.

3.10.4 Reciprocity will not be granted if the following conditions apply:

a. The individual has more than 24 months break in service; or

b. A favorable adjudication is more than five years old; or

c. The agency obtains new information that calls into question the individual's continued eligibility for access to CNSI.

3.11 Access to Restricted Data (RD) or Formerly Restricted Data (FRD

3.11.1 Access to Restricted Data (RD) and Formerly Restricted Data (FRD) outside the scope of aeronautical and space activities require clearance by the Department of Energy (DOE) or the Nuclear Regulatory Commission (NRC).

3.11.2 If such access is required solely for the performance of service for another agency, that agency normally shall initiate the required investigation. In such a case, the OPM reimbursable investigation required for the occupant of a sensitive position will not be initiated.

3.11.3 The Central Adjudication Facility (CAF) shall assist the other agency by obtaining and providing the required security documents.

3.11.4 When access to RD or FRD outside the scope of aeronautical and space activities are required in the performance of NASA duties, a request for either a DOE or an NRC clearance shall be initiated by the CCS/CCPS, who will forward the necessary documents to the Special Security Officer for appropriate action.

3.12 Guiding Principles for Adjudication, Suspension, Denial, or Revocation of Security Clearances

3.12.1 The Adjudicative Guidelines for Determining Eligibility for Access to Classified Information serve as a guide for investigators and adjudicators to identify potential issues that may adversely affect an individual's eligibility for access to classified information.

3.12.2 Only the AA, OPS, or his designee shall deny or revoke a security clearance.

3.12.3 The AA, OPS, and CCS/CCPS may suspend security clearances.

3.12.4 Adjudications shall be fully documented and recorded in the subject's security file and entered into the NASA Clearance Tracking System (NCTS).

3.12.5 Information developed during the investigation process for a security clearance may not be shared with the Center OHCM or management while the investigation is pending. The AA, OPS or CCS/CCPS may override this principle, if in their judgment the information suggests that the subject poses an immediate and serious threat to the health or safety of other individuals, is a threat to a critical mission, or shall otherwise be ineligible for or lose continuation of Federal employment.

3.12.6 All reasonable efforts shall be pursued to fully develop potential issue information, as well as potentially favorable or mitigating information.

3.12.7 The CCS/CCPS will propose suspensions of security clearances to the NASA CAF for cause based on developed adverse information. The AA, OPS, will make final denial or revocation determinations after consultation with the NASA CAF and Office of General Counsel personnel.

3.12.8 Requests for a security clearance shall result in an adjudicative determination unless, unrelated to any potential adjudication factor, the need for the security clearance no longer exists, such as severance of the subject's employment.

3.12.9 Subjects of adjudication are allowed to refute any information developed during the investigation process that may make the person ineligible for access to classified information.

3.12.10 In the event of a denial or revocation of a security clearance, the subject is entitled to obtain a review of the decision.

3.12.11 Center OHCM personnel, in coordination with security office personnel and supervisors, will make employment suitability determinations. The Center OHCM shall coordinate and document those determinations.

They are separate and distinct from security clearance adjudications.

3.12.12 The policies and the procedures for the suspension, denial, and revocation of a security clearance shall not be confused with the procedures for the removal of an employee on national security grounds as set forth in 5 U.S.C. § 7532, Suspension and Removal. A CCS/CCPS may coordinate with OHCM to pursue the removal of an employee on national security grounds, regardless of the sensitivity of the employee's position or whether the employee has access to classified information.

3.13 Bond Amendment

3.13.1 The Bond Amendment 50 U.S.C. § 435c (b) repealed the Smith Amendment 10 U.S.C. § 996, and places restrictions that are similar to the Smith Amendment, but which apply to all Federal Government agencies. The Bond Amendment bars persons from holding a security clearance for access to Special Access Programs, Restricted Data, and SCI if they have been:

a. Convicted of a crime and served more than one year of incarceration.

b. Discharged from the Armed Forces under dishonorable conditions.

c. Determined to be mentally incompetent by a court or administrative agency.

3.13.2 The Bond Amendment also prohibits all Federal agencies from granting or renewing a security clearance for any covered person who is an unlawful user of controlled substance(s) or is an addict; this prohibition applies to all clearance holders.

3.14 Adjudication of Security Clearances

3.14.1 The AA, OPS, and the NASA CAF adjudicators are empowered to determine an employee's security clearance eligibility.

3.14.2 Each investigation required for a specific clearance level will be complete with sufficient scope in order to appropriately adjudicate for access to classified information.

3.14.3 In instances when management, for reasons unrelated to the adjudicative process, withdraws a request for a security clearance and the subject of the investigation continues his or her employment with NASA, potential issue information developed during the investigative process will be made available to OHCM to make a suitability determinations.

3.14.4 The initial adjudication will be made once the adjudicator has gathered all available pertinent information.

3.14.5 The senior adjudicator shall review the initial adjudication for fairness, completion, and proper application of the adjudication guidelines.

3.15 Suspension of Security Clearances

3.15.1 The AA, OPS, Center Director, or the CCS/CCPS shall suspend an individual's security clearance when information is developed that suggests the individual's continued access to classified information is not in the interest of national security. The determination to suspend should be based on thorough review of definitive derogatory information. All suspensions will be reported immediately to the Central Adjudication Facility by way of the NASA Clearance Tracking System.

a. The subject shall be notified accordingly. However, the reason or reasons for a suspension need not be provided to the subject of a suspension.

b. Suspension of a security clearance shall not be open-ended. Every effort should be expended to complete the investigation and to adjudicate as soon as practical. All suspension actions should be resolved as soon as practical from the date of the suspension.

c. Suspension of an individual's access to classified information is not an adverse action. Suspension merely allows the agency time to investigate and adjudicate information that may affect the individual's eligibility for access to classified information.

d. A suspension is a temporary status. The subject of a suspension is not entitled to the review procedures required for denial or revocation of a security clearance. e. Upon receipt of suspension information containing documented facts that fully support the suspension, CAF personnel will determine whether to reinstate or revoke the clearance of the individual.3.16 Denial or Revocation of Security Clearances

3.16.1 No individual will be given access to classified information or assigned to a sensitive position unless a favorable security eligibility determination has been made. In the event of an unfavorable adjudication action, the NASA CAF shall propose documented reasons in a Letter of Intent (LOI) to deny or revoke a clearance.

3.16.2 The Director, Security Management Division (DSMD) shall review the proposed unfavorable adjudicative action by CAF personnel and:

a. Remand the case for further work; or

b. Uphold the proposed adjudication of the information, and in consultation with the Office of General Counsel, provide written notice to the subject of the denial of the revocation of the security clearance through the CCS/CCPS.

3.16.3 The employee shall acknowledge receipt of the LOI and determine whether he/she intends to respond within the time specified in the LOI. If the subject provides new information for consideration, CAF personnel shall review the new information provided. CAF personnel will make a recommendation to the DSMD whether a security clearance should be reinstated, revoked, or denied. If inadequate or no information is provided or no response is provided within the specified time allowed, CAF personnel will continue with the denial or revocation process. Upon completion of the process, the subject will be notified by the DSMD of a final decision in a Letter of Notification (LON). The letter is served through the CCS/CCPS.

3.16.4 If the subject receives a LON of denial or revocation, the subject will be afforded an opportunity to appeal the LON to the AA, OPS. If at any point, the employee alleges the clearance determination is contemplated or made in retaliation for a protected disclosure defined within the Presidential Policy Directive (PPD-19), the employee's case will be reviewed by the Office of Inspector General, as it separately prescribes. Where this review is requested, in his sole discretion, the AA OPS may await the OIG review of the employee's case prior to making a security clearance determination, or may take action to suspend, revoke, or otherwise restrict the employee's clearance. Any report provided by the OIG will be carefully considered by AA OPS, including consideration of reinstating a revoked or suspended clearance.

3.16.5 The AA, OPS, shall ensure that the rights of the subject are protected and due process is accorded, including the opportunity for the subject to appear in person to present relevant documents, materials, and information prior to final determination by the AA, OPS. If the employee takes advantage of the opportunity to appear personally before the AA, OPS, the AA, OPS will document such appearance by means of a written summary or recording which will be made a part of the subject's security record.

3.16.6 If the AA, OPS, provides a notice of denial or revocation and the subject subsequently requests an appeal by a Security Adjudication Review Panel (SARP), the NASA Administrator will appoint that body. The panel will be composed of three NASA employees who have demonstrated reliability and objectivity in their official duties. Panel members will have a favorable SSBI, and only one of the panel members may be a security professional. If use of a NASA security professional is not appropriate, a security expert from outside the Agency may be used on the panel. The subject may submit a written appeal to the SARP or they may choose to appeal in person to the SARP. Any personal appearance before the SARP will be documented by means of a written summary or recording which will be made a part of the subject's security record.

3.16.7 Prior to finalizing the SARP determination, a SARP panel member or the AA, OPS, may refer the SARP proposed decision to the Administrator for an additional level of review. If no referral is made to the Administrator, the SARP decision is final. If there is a referral to the Administrator, the Administrator's decision is the final agency decision.

3.16.8 An employee subject to a clearance denial, suspension, or revocation action (including having received an LOI or LON), may allege reprisal and/or retaliation for making a protected disclosure, or for participating in same (such as a witness). If so, that employee's case shall be forwarded to the OIG for its review, under procedures as it may separately prescribe. Any OIG report will be carefully considered by the AA OPS. An employee alleging reprisal who has exhausted the internal NASA appeal process (including review by the NASA OIG) may request an external review by a three-member Inspector General panel, which may be granted per PPD-19 section C in the sole discretion of the Inspector General of the Intelligence Community. The Administrator shall carefully consider the findings of and actions recommended by any external review panel. Accordingly, NASA may suspend or revoke a clearance pending either the NASA OIG review or the external review panel, understanding that the employee may be reinstated and compensated for damages of an improper clearance denial, suspension, or revocation.

3.16.9 Upon determination that a clearance revocation or denial has been upheld, the case then becomes one of employment suitability and shall be referred to OHCM for suitability determination.

3.17 Continuous Evaluation of Security Clearance Eligibility

3.17.1 A personnel security clearance determination is based on a continuous assessment of an individual's personal and professional history, demonstrated loyalty to the United States, strength of character, trustworthiness, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential coercion and willingness to abide by regulations governing the use, handling, and protection of CNSI.

3.17.2 In order to ensure that all persons who have been granted a security clearance remain eligible, all U.S. Government clearance holders shall be subject to a continuous evaluation of their qualifications to meet the high standards of conduct expected of persons in national security positions.

3.17.3 Persons subject to a prior favorable personnel security determination who demonstrate behavior that places doubt on their loyalty, reliability, or trustworthiness or otherwise disqualifies that individual for continued eligibility for a security clearance shall be subject to further scrutiny and possible suspension of access to CNSI.

3.17.4 Center Directors and the CCS/CCPS shall ensure that a program of continuous evaluation for security clearance eligibility is developed that relies on all levels of management and all security clearance holders to be aware of the standards of conduct for qualification to hold a security clearance and their responsibility to report adverse behavior that is disqualifying. Where employees have significant involvement with handling, storing, marking, or exercising original or derivative classification of CNSI, supervisors will include these responsibilities as a critical element of the employees' annual performance communication system documentation.

3.17.5 Supervisors and managers are critical to the success of the Continuous Evaluation Program. Supervisors shall report incidents of potentially disqualifying behavior that they are aware of to the CCS/CCPS and be observant to potential changes in behavior of their subordinates that could cause potential risk to the CNSI to which the employee has been entrusted.

3.17.6 Holders of security clearances and other employees with knowledge that an employee holds a security clearance shall be advised and periodically reminded to report to their supervisor or appropriate security officials when they become involved in behavior or become aware of such behavior of another cleared individual that could impact their continued eligibility for access to CNSI. A security clearance holder who fails to report disqualifying conduct involving other cleared personnel is also subject to suspension of access to CNSI, pending a security inquiry.

3.17.7 CCS/CCPS should conduct fact finding of reports of disqualifying conduct, and depending on the adverse

impact to national security, may suspend an individual's access to CNSI for cause. CCS/CCPS may request a periodic assessment or other PSI to support their assessment of the employees' continued access to classified information. CCS/CCPS will forward a report to the NASA CAF personnel as soon as possible after fact finding. CAF personnel will determine if the individual continues to be eligible for access to CNSI.

3.18 Classified Visits and Meetings

3.18.1 Classified visits to other agencies. Employees who have a need to certify their security clearance should contact their Center security office.

a. An inter-agency clearance verification request can be generated by the security office upon review of the NCTS and then forwarded to the facility or custodian.

b. The request may be completed by the personnel security specialist or special security officer who has access to NCTS.

c. Visit requests are normally issued for no more than one year at a time. Visit requests for longer than one-year are at the discretion of the agency being visited. A copy shall be maintained in the security file for record.

3.18.2 Classified visit requests and classified meetings. Employees hosting meetings involving classified information will advise the prospective attendees to have their agency security office prepare and transmit certifications of the attendees' security clearances to the respective Center personnel security office or the special security officer. The certifications should include the investigation record information used as a basis to grant the clearance, Center point of contact, purpose, and duration of the visit. If these certifications are not forwarded, then custodians of the classified materials may verify the clearances of attendee's in OPM's PIPS/CVS system. Clearances from agencies that cannot be verified in the PIPS/CVS system will require a certification of clearance from the agency.

3.18.3 Special Access Program (SAP) Visits. All visit requests involving special access programs shall be processed by the appropriate special security office.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS